UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SCOTT GLABB on behalf of himself and all others similarly situated, Plaintiff, v. **PENSION BENEFITS INFORMATION, LLC,** Defendant.	**Case No.** **CLASS ACTION** **COMPLAINT FOR:** **(1) NEGLIGENCE** **(2) VIOLATION OF THE CAL. CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.150** **(3) VIOLATION OF THE CAL. CUSTOMER RECORDS ACT, CAL. CIV. CODE § 1798.84** **(4) VIOLATION OF THE CAL. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200** **(5) VIOLATION OF THE RIGHT TO PRIVACY, CAL. CONST. ART. 1, § 1** **(6) BREACH OF IMPLIED CONTRACT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Scott Glabb ("Plaintiff"), by and through his undersigned counsel, individually and on behalf of all similarly situated persons, alleges the following against Pension Benefits Information, LLC and any affiliates (collectively, "PBI" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. This putative class action arises from PBI's negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach of its systems, which was discovered in May or June 2023 (the "Data Breach").

2. PBI acts as a third- party provider of pension management services to public pensions throughout the nation, including the California Public Employees' Retire System ("CalPERS") and the California Teachers' Retirement Fund ("CalSTRS").

3. In connection with the Data Breach, PBI failed to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information, including without limitation, full names, dates of birth, and Social Security numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as "personal identifiable information" or "PII").[1]

4. The Data Breach has impacted more than 700,000 CalPERS members and an unknown number of CalSTRS members.[2]

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] *See* https://www.sacbee.com/news/politics-government/capitol-alert/article276638381.html (last visited on July 27, 2023)

5. The Data Breach has also impacted several million additional individuals nationwide for whom PBI provides pension and insurance related services.[3]

6. Plaintiff brings this class action complaint to redress injuries related to the Data Breach, on behalf of himself and a nationwide class and California subclass of similarly situated persons.

7. Plaintiff asserts claims on behalf of a nationwide class for negligence, negligence per se, declaratory judgment, common law invasion of privacy, breach of implied contract and breach of implied covenant of good faith and fair dealing.

8. Plaintiff also brings claims on behalf of a California subclass for violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, the California Customer Records Act, Cal. Civ. Code § 1798.80 et seq., violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., and for invasion of privacy based on the California Constitution, Art. 1, § 1.

9. Plaintiff seeks, among other things, compensatory damages, injunctive relief, attorneys' fees, and costs of suit.

10. Plaintiff further intends to amend this complaint to seek statutory damages on behalf of the California subclass upon expiration of the 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b).

[3] *See* https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/ (last visited on July 27, 2023).

II. PARTIES

11. Plaintiff Scott Glabb is, and at all times mentioned herein was, a citizen and resident of the State of California whose PII was part of the June 2023 Data Breach that is the subject of this action.

12. On information and belief, Defendant Pension Benefit Information, LLC is a Delaware limited liability corporation with its principal place of business located at 333 S. 7th Street, Suite 2400, Minneapolis, Minnesota 55402.

13. Plaintiff brings this action on behalf of herself, on behalf of the general public as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

III. JURISDICTION AND VENUE

14. This Court has general personal jurisdiction over PBI because, at all relevant times, PBI had systematic and continuous contacts with the State of Minnesota. PBI does business in Minnesota, and has offices in Minneapolis, Minnesota. Defendant regularly contracts with a multitude of businesses, organizations and consumers in Minnesota to provide pension plan management services. PBI does in fact actually provide such continuous and ongoing pension plan management services to such customers in Minnesota and has employees in Minnesota.

15. Furthermore, this Court has specific personal jurisdiction over PBI because the claims in this action stem from its specific contacts with the State of Minnesota — namely, PBI's provision of pension plan management services to a multitude of clients in

Minnesota, PBI's collection, maintenance, and processing of the personal data of Minnesotans in connection with such services, including but not limited to PBI's employees, PBI's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data in June 2023.

16. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the mater in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the PBI, including Plaintiff.

17. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court pursuant to 28 U.S.C. § 1367.

18. Venue is proper in the District of Minnesota under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically PBI's provision of pension plan management services in Minnesota and within Minneapolis specifically, PBI's collection, maintenance, and processing of the personal data of Minnesotans in connection with such services, PBI's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent security breach of such data in June 2023 through a vulnerability on a secure file transfer application hosted by PBI in his District, which vulnerability and subsequent security breach resulted from PBI's failures, as alleged herein. In addition, Plaintiff is informed and believes and thereon alleges that PBI has offices within the District of Minnesota.

IV. FACTUAL ALLEGATIONS

A. PBI's Business and Collection of Plaintiff's and Class Members' Private Information

19. PBI provides pension benefit management services to public pensions throughout the nation, including CalPERS and CalSTRS.

20. The California Public Employees' Retirement System, or "CalPERS," is the largest public pension fund in the United States, with over $400 billion in its portfolio.

21. The California Teachers' Retirement Fund, or "CalSTRS," is a sister fund to CalPERS, and has more than $300 billion in its portfolio.

22. PBI is a third-party contractor for CalPERS and CalSTRS, providing necessary pension management services. For example, PBI performs critical work of identifying pension members who have died. As part of this work, PBI prevents overpayment of pension benefits and helps identify beneficiaries who are entitled to continued pension benefits.

23. In connection with its pension management services, PBI collects, stores, and processes sensitive personal data for thousands of individuals, including but not limited to pension members for whom PBI is providing management services. In doing so, PBI retains sensitive information including, but not limited to, bank account information, addresses, driver's license numbers, dates of birth, and social security numbers, among other things.

24. As a pension management business involving California public pension members, PBI is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

25. PBI knew that it was a prime target for hackers given the significant amount of sensitive personal information processed through its computer data and storage systems. PBI's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

26. Despite knowing the prevalence of data breaches, PBI failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. PBI has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. PBI failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

27. Specifically, on or around June 6, 2023, PBI notified CalPERS that it discovered a significant cybersecurity breach that occurred at an unknown time. PBI notified CalPERS that a vulnerability in the MOVEit transfer application allowed data to be downloaded by an unauthorized third party – a vulnerability that, upon information and belief, PBI was aware of yet failed to address in a timely fashion, leading to the Data Breach. Very few specific details about the Data Breach have been provided to impacted individuals.

28. On information and belief, the personal information PBI collects (and which was impacted by the Data Breach) includes individual's name, date of birth, and social security number, among other personal, sensitive and confidential information.

29. On or around June 26, 2023, CalSTRS mailed data breach notices to impacted parties, including Plaintiff. According to notice mailed to impacted individuals, the breach resulted in individual's names, social security numbers, dates of birth, and ZIP codes being compromised and acquired by unauthorized actors. Plaintiff received a copy of the June 26, 2023 data breach notice via United States mail service confirming that his personal identifying information was part of the Data Breach.

30. Upon information and belief, the hackers responsible for the Data Breach downloaded and stole the PII impacted in the Data Breach. Because of the nature of the Data Breach and of the personal information stored or processed by PBI, Plaintiff is informed and believes that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed and believes that criminals would have no purpose for hacking PBI other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by PBI.

31. The personal information exposed by PBI as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law

enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

32. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

33. The information compromised in the PBI Data Breach involves sensitive personal identifying information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—particularly social security numbers.

34. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

35. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

36. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

$200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

37. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

38. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[4] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-datasold-on-the- dark-web-how-much-it-costs/ (last visited on July 27, 2023).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-howmuch-your-. personal-information-is-selling-for-on-the-dark-web/ (last visited on July 27, 2023).

[6] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on July 27, 2023).

39. Identity thieves can use PII, such as that of Plaintiff and Class Members (which PBI failed to keep secure) to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

40. The ramifications of PBI's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Indeed, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

[7] Report to Congressional Requesters, GAO, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited on July 27, 2023).

42. When cyber criminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

43. And data breaches are preventable.[8] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[9] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[10]

44. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[11]

45. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

---

[8] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[9] *Id*. at 17.
[10] *Id*. at 28.
[11] *Id*.

46. According to the FTC, the need for data security should be factored into all business decision-making.[12] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[13] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

47. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[14]

48. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to

[12] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on July 27, 2023).
[13] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0136_proteting-personal-information.pdf (last visited on July 27, 2023).
[14] *See id.*

adequately and reasonably protect personal information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act" or "FTCA"), 15 U.S.C. § 45.

49. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that compiles already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled *How to Protect Your Networks from Ransomware* and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.[15] Preventative measures include:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[15] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/filerepository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited on July 27, 2023)

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

[16] *Id.*

51. PBI could have prevented the Data Breach by properly utilizing best practices as advised by the federal government and described in the preceding paragraphs but failed to do so.

52. PBI's failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as PBI that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, PBI knew or should have known that it was a prime target for hackers.

53. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[17]

54. Upon information and belief, PBI did not encrypt Plaintiff's and Class Members' personal information involved in the Data Breach.

55. Despite knowing the prevalence of data breaches, PBI failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized

[17] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, Security, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-oforganizations-have-suffered-a-cloud-based-datq-breach (last visited on July 27, 2023).

access to its highly sensitive systems and databases. PBI has the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. PBI failed to fully implement each and all of the above-described data security best practices. PBI further failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

56. As detailed above, PBI is a large, sophisticated pension benefits management company with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

57. PBI disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

B. PBI Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

58. In addition to its obligations under federal laws and regulations, PBI owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal information from being compromised, lost, stolen, accessed, and misused by unauthorized persons. PBI owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, adequate monitoring of its employees, agents, and vendors, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

59. PBI breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly monitor, maintain and safeguard its Plaintiff's and Class Members' Private Information. PBI's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect Plaintiff's and Class Members' PII;

b. Failing to sufficiently monitor its employees, agents, and vendors regarding the proper handling of Plaintiff's and Class Members' PII;

c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

60. Accordingly, Plaintiff's and Class Members' lives were severely disrupted by the Data Breach. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

C. Plaintiff's and Class Members' Damages

61. PBI received highly sensitive PII from Plaintiff in connection with PBI's provision of pension benefit management services the company provided to CalSTRS.

62. As a result of PBI's provision of pension management services on behalf of CalSTRS, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

63. At all times herein relevant, Plaintiff is and was a member of the nationwide class and the California subclass alleged herein.

64. Plaintiff's PII was exposed in the Data Breach because PBI stored and/or controlled Plaintiff's PII at the time of the Data Breach.

65. Plaintiff received a letter from CalSTRS, dated June 26, 2023, stating that his name, social security number, date of birth, and ZIP code that were in the possession, custody and/or control of PBI was involved in the Data Breach.

66. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include, signing up for Defendant's offered credit monitoring and identity theft insurance; changing passwords and resecuring his own

computer network; self-monitoring his accounts for any indication of fraudulent activity, which may take years to detect; and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

67. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to PBI, which was compromised in and as a result of the Data Breach.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII.

69. Plaintiff further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails since the Data Breach.

70. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name and Social Security number being placed in the hands of unauthorized third parties/criminals.

71. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in PBI's possession, is protected and safeguarded from future breaches.

72. Plaintiff's and Class Members' personal identifying information, including their names and social security numbers, were in the possession, custody and/or control of

PBI. Plaintiff believed that PBI would protect and keep his personal identifying information protected, secure and safe from unlawful disclosure.

73. Plaintiff and Class Members have spent and will continue to spend time and effort monitoring their accounts to protect themselves from identity theft. Plaintiff and Class Members remain concerned for their personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

74. As a direct and foreseeable result of PBI's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff and Class Members have suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach.

75. Plaintiff and Class Members are especially concerned about the misappropriation of their Social Security numbers. Social security numbers are among the most sensitive kind of personal information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's social security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use

> the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

76. Furthermore, Plaintiff and Class Members are well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, Plaintiff and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach. Additionally, Plaintiff and Class Members have incurred, and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

V. CLASS ACTION ALLEGATIONS

77. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

78. Specifically, Plaintiff proposes the following Nationwide Class and California Subclass (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

[18] *See* Identify Theft and Your Social Security Number, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited on July 27, 2023).

California Subclass

All individuals residing in the state of California who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

79. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

80. Plaintiff reserves the right to modify or amend the definitions of the proposed Class, as well as add additional subclasses, before the Court determines whether certification is appropriate.

81. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

82. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of hundreds of thousands of individuals whose PII was in the possession and control of PBI and later compromised in the Data Breach. The identities of Class Members are ascertainable through PBI's records, Class Members' records, publication notice, self-identification, and other means.

83. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether PBI engaged in the conduct alleged herein;

b. When PBI actually learned of the MOVEit vulnerability and resulting Data Breach;

c. Whether PBI's response to the Data Breach was adequate;

d. Whether PBI unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether PBI failed to implement and maintain reasonable monitoring and supervisory procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether PBI adequately ensured that its data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether PBI owed a duty to Class Members to safeguard their Private Information;

h. Whether PBI breached its duty to Class Members to safeguard their Private Information;

i. Whether hackers acquired and obtained Class Members' Private Information via the Data Breach;

j. Whether PBI knew or should have known that its data security systems were deficient;

k. What damages Plaintiff and Class Members suffered as a result of PBI's misconduct;

l. Whether PBI's conduct was negligent;

m. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

n. Whether Plaintiff and Class Members are entitled to additional credit and identity monitoring and monetary relief;

o. Whether PBI's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200;

p. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and the California Consumer Privacy Act, Civ. Code § 1798.150, and the proper measure of such damages, and/or statutory damages pursuant § 1798.150(a)(1)(A) and the proper measure of such damages; and

q. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

84. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

85. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

86. Predominance. PBI has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from PBI's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

87. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PBI. In contrast, conducting this

action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

88. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). PBI has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

89. Finally, all members of the proposed Class are readily ascertainable. PBI has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PBI.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Class)

90. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

91. PBI owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons.

92. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices.

93. PBI's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiff's and Class Members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its clients, Plaintiff, and Class Members of any data breach.

94. PBI's duties to use reasonable care arose from several sources, including but not limited to those described below.

95. PBI had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but PBI also knew that it was more likely than not Plaintiff and other Class Members would be harmed.

96. PBI's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as PBI.

97. Various FTC publications and data security breach orders further form the basis of PBI's duty. According to the FTC, the need for data security should be factored

into all business decision making.[19] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[20] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

98. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

99. The FBI has also issued guidance on best practices with respect to data security that also form the basis of PBI's duty of care, as described above.21

[19] *See Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on July 27, 2023).
[20] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last visited on July 27, 2023).

100. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' personal information, PBI assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' personal information from disclosure.

101. PBI also had a duty to safeguard the personal information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require PBI to reasonably safeguard personal information, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq*.

102. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by PBI's misconduct.

103. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their personal information.

104. PBI breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. PBI breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiff and Class Members; (b)

prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiff's and Class Members' personal information in PBI's possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

105. PBI knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of PBI's operations further shows that PBI knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued PBI's systems and led to the data breach.

106. Through PBI's acts and omissions described in this complaint, including PBI's failure to provide adequate security and its failure to protect the personal information of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, PBI unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' personal information.

107. PBI further failed to timely and accurately disclose to clients, Plaintiff, and Class Members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web. Plaintiff and Class Members could have taken action to protect their personal information if they were provided timely notice.

108. But for PBI's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their personal information would not have been compromised.

109. Plaintiff and Class Members relied on PBI to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

110. As a direct and proximate result of PBI's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory and nominal damages, in an amount to be proven at trial. As a result of PBI's failure to protect Plaintiff's and Class Members' personal information, Plaintiff's and Class Members' personal information has been accessed by malicious cybercriminals. Plaintiff 'and the Class Members' injuries include:

a. theft of their personal information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

d. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

e. damages to and diminution of value of their personal information entrusted, directly or indirectly, to PBI with the mutual understanding that PBI would safeguard Plaintiff's and the Class Members' data against theft and not allow access and misuse of their data by others;

f. continued risk of exposure to hackers and thieves of their personal information, which remains in PBI's possession and is subject to further breaches so long as PBI fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the Data Breach;

g. loss of the inherent value of their personal information;

h. the loss of the opportunity to determine for themselves how their personal information is used; and

i. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

111. In connection with the conduct descried above, PBI acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class Members would suffer if their highly sensitive and confidential personal information, including but

not limited to name, company name, address, social security numbers, and banking and credit card information, was access by unauthorized third parties.

COUNT II
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE §§ 1798.100 *ET SEQ.*, § 1798.150(A)
(On behalf of Plaintiff and the California Subclass)

112. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

113. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

114. PBI is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

115. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

116. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information PBI collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

117. PBI knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. PBI failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California

Subclass Members. Specifically, PBI subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the PBI's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

118. As a direct and proximate result of PBI's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass Members' personal information included exfiltration, theft, or disclosure through PBI's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

119. As a direct and proximate result of PBI's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

120. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the California Subclass Members by way of this complaint seek actual pecuniary damages suffered as a result of PBI's violations described herein. Plaintiff issued a notice of these alleged violations pursuant to § 1798.150(b) and intends to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

COUNT III
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE §§ 1798.80 *ET SEQ*.
(On behalf of Plaintiff and the California Subclass)

121. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

122. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

123. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

124. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

125. Plaintiff and the California Subclass Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to PBI, directly and/or indirectly, for the purpose of obtaining a service from PBI.

126. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information PBI collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

127. PBI knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. PBI failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, PBI failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass Members from unauthorized

access, destruction, use, modification, or disclosure. PBI further subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the PBI's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

128. As a direct and proximate result of PBI's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass Members by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

129. As a direct and proximate result of PBI's acts or omissions, Plaintiff and the California Subclass Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

130. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal

information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

131. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

132. PBI failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, PBI has not sent written notice of the data breach to all impacted individuals. As a result, PBI has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the Data Breach, members could have taken action to protect their personal information but were unable to do so because they were not timely notified of the breach.

133. On information and belief, many California Subclass Members affected by the breach have not received any notice at all from PBI in violation of Section 1798.82(d).

134. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

135. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their

identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT IV
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200 *ET SEQ.*
(On behalf of Plaintiff and the California Subclass)

136. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

137. PBI is a "person" defined by Cal. Bus. & Prof. Code § 17201.

138. PBI violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

139. PBI's "unfair" acts and practices include:

a. PBI failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the PBI Data Breach.

b. PBI failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

c. PBI's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

d. PBI's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of PBI's inadequate security, consumers could not have reasonably avoided the harms that PBI caused; and

e. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

140. PBI has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

141. PBI's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable data security and privacy measures to protect Plaintiff's and California Subclass Members' personal information, which was a direct and proximate cause of the PBI Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the PBI Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the PBI Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

142. PBI's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PBI's data security and ability to protect the confidentiality of consumers' personal information.

143. As a direct and proximate result of PBI's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

144. PBI's violations were, and are, willful, deceptive, unfair, and unconscionable.

145. Plaintiff and California Subclass Members have lost money and property as a result of PBI's conduct in violation of the UCL, as stated herein and above.

146. By deceptively storing, collecting, and disclosing their personal information, PBI has taken money or property form Plaintiff and California Subclass Members.

147. PBI acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass Members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

148. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from PBI's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT V
COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On behalf of Plaintiff and the Class)

149. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

150. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

151. PBI intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class Members by intentionally configuring their systems in such a way that

left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class Members' personal information. Only PBI had control over its systems.

152. PBI's conduct is especially egregious and offensive as it failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class Members' personal information.

153. At all times, PBI was aware that Plaintiff's and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

154. Plaintiff and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

155. PBI intentionally configured their systems in such a way that stored Plaintiff's and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and Class Members' privacy interests.

156. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiff and Class Members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

157. PBI's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive

information, in addition to social norms. PBI's conduct would be especially egregious to a reasonable person as PBI publicly disclosed Plaintiff's and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," *i.e.*, hackers.

158. As a result of PBI's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

159. Plaintiff and Class Members have been damaged as a direct and proximate result of PBI's intrusion upon seclusion and are entitled to just compensation.

160. Plaintiff and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

COUNT VI
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

161. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

162. Through its course of conduct, PBI, Plaintiff and Class Members entered into implied contracts for PBI to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

163. PBI required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services for pension management services through CalPERS and/or CalSTRS.

164. PBI solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant for pension management services through CalPERS and/or CalSTRS.

165. Plaintiff and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

166. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

167. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

169. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the

stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and California Subclass requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing PBI to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring PBI to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 27, 2023

Respectfully submitted,

/s/ *Bryan L. Bleichner*
Bryan L. Bleichner (MN BAR #0326689)
Philip J. Krzeski (MN BAR #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbliechner@chestnutcambronne.com

Mason A. Barney (*pro hac vice* forthcoming)
Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: mbarney@sirillp.com
Email: tbean@sirillp.com